

## Bonusaufgabe Rainbow-Table

---

Erstellen Sie mit Java eine Rainbow-Table für MD5 ausgehend von den ersten 2.000 Passwörtern der Länge 7 bestehend aus Kleinbuchstaben und Ziffern. (Also von 0000000, ... 0000009, 000000a, 000000b, ..., 000000z, 0000010, ...). Die Kettenlänge soll 2000 betragen, es soll also jeweils 2000 mal die Hashfunktion und die entsprechende Reduktionsfunktion angewendet werden. Verwenden Sie als Reduktionsfunktion die auf Folie 3.27 angegebene Konstruktion mit der Menge  $Z = \{0, 1, \dots, 9, a, b, \dots, z\}$ .

Ermitteln Sie mit der Tabelle und dem Algorithmus aus der Vorlesung (insbesondere dürfen Sie **nicht** bei der Erstellung der Tabelle "mitlauschen") den Klartext zu dem in Hexadezimal-Schreibweise angegebenen Hashwert 1d56a37fb6b08aa709fe90e12ca59e12 oder begründen Sie, dass dies mit der zu konstruierenden Rainbow-Table nicht möglich ist.

### Hinweise:

- Sie können in Gruppen von bis zu drei Personen arbeiten.
- Schreiben Sie ein **kommentiertes** Programm.
- Zur Kontrolle: Die erste Kette beginnt so:  
0000000  
29c3eea3f305d6b823f562ac4be35217  
87inwgn  
12e2feb5a0feccf82a8d4172a3bd51c3  
frrkiis  
437988e45a53c01e54d21e5dc4ae658a  
dues6fg  
c0e9a2f2ae2b9300b6f7ef3e63807e84  
und so weiter.
- Bei Zusendung des Programms (der Quellcode reicht) bis zum **30.04.2025** erhalten Sie einen Bonus von 0.3 auf die Note des zweiten Tests. (Aus systemtechnischen Gründen kann aber die Erfahrungsnote am Ende nicht > 6 sein.)
- **Schicken Sie das Resultat ihres Programms in ihrer Mail als Screenshot mit!**
- Beachten Sie, dass es sich um Bonuspunkte handelt. Damit können sich interessierte Studierende durch Zusatzarbeit einen kleinen Bonus verdienen. Eigentlich gehe ich davon aus, dass Sie aus Fairnessgründen diesen Studierenden gegenüber nicht versuchen, zu betrügen. Dennoch werde ich dies (auch mit Hilfe von Tools) kontrollieren. Falls dabei ein Täuschungsversuch festgestellt wird (also: (verschleierte) Kopien von Teilen existierender Programme), wird die Note des nächsten Tests auf 1.0 gesetzt.